Tina Wolfson, CA Bar No. 174806
twolfson@ahdootwolfson.com
Theodore Maya, CA Bar No. 223242
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Telephone: (310) 474-9111
Fax: (310) 474-8585

Daniel S. Robinson, CA Bar No. 244245
drobinson@robinsonfirm.com
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

IN RE EXPERIAN DATA BREACH LITIGATION

No. SACV 15-1592 AG (DFMx)

PLAINTIFFS' NOTICE OF MOTION AND MOTION TO COMPEL PRODUCTION OF DEFENDANT'S DATA BREACH REPORT; MEMORANDUM OF POINTS AND AUTHORITIES

Date: May 15, 2017
Time: 10:00 a.m.
Room: Court 10D

Hon. Andrew J. Guilford, presiding

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on May 15, 2017, at 10:00 a.m., or as soon thereafter as the matter may be heard before the Honorable Andrew J. Guilford in Courtroom 10D of the above entitled Court located at 751 W. Santa Ana Blvd., Santa Ana, CA 92701, Plaintiffs will and hereby do move for an order compelling production of the following documents, as they are identified on Defendant's Supplemental Privilege Log (Declaration of Theodore Maya Ex. A): P000002-3; P000005-6; P000008-9; P000011-15; P000017-18; P000020-23; P000025-26; P000028-31; P000033-37; P000039-40; P000042-44; P000046-48; P000050-54; P000056-58; P000060-63; P000065-67; P000069-70; P000072-73; P000077-78; P000080-81; P000083-84; P000086-90; P000092-93; P000095-96; P000098-100; P000102-03; P000105-06; P000108; P000110-11; P000113-24; P000126-74; P000177-88; P000190-91; P000193-97; P000199-216; P000218-223; P000225-29; P000231-34; P000236-37; P000239-40; P000242-45; P000248; P000250-54; P000256-57; P000259-60; P000262; P000264-70; P000272-75; P000278-84; P000286-92; P000294-99; P000302-16; P000318-20; P000322; P000324-25; P000327-28; P000330-31; P000333-34; P000337-39; P000342-44; P000346-47; P000349-51; P000353; P000355-57; P000359-62; P000364-66; P000371; P000373-79; P000381-84; P000386-90; P000392-93; P000395-96; P000398-400; and P000402-07.

Plaintiffs further request that the Court conduct an *in camera* review of the following 28 documents, as they are identified on Defendant's Supplemental Privilege Log, in order to assess Defendant's claims of privilege with respect to them: P000075; P000175-76; P000189; P000192; P000198; P000249; P000255; P000258; P000277; P000285; P000293; P000323; P000329; P000332; P000335-36; P000340-41; P000354; P000358; P000363; P000367-70; P000394; and P000397.

This Motion is based on Federal Rules of Civil Procedure 26 and 37, this Notice of Motion, the accompanying Memorandum of Points and Authorities, the Declaration of

Matthew Strebe ("Strebe Decl."), the Declaration of Theodore Maya ("Maya Decl."), the [Proposed] Order, all documents on file in the above-referenced matter, the arguments presented by counsel at the requested hearing, and any other matter the Court wishes to consider.

This motion is made following the conference of counsel pursuant to L.R. 7-3 which took place between approximately May 2016 and February 2017.

Dated: April 12, 2017

Respectfully submitted,

/s/ Theodore Maya
Theodore Maya

AHDOOT & WOLFSON, P.C.
Tina Wolfson
twolfson@ahdootwolfson.com
Theodore Maya
tmaya@ahdootwolfson.com
1016 Palm Avenue
West Hollywood, CA 90069
Telephone: 310-474-911
Fax: 310-474-8585

ROBINSON CALCAGNIE ROBINSON SHAPIRO DAVIS, INC.

/s/ Daniel S. Robinson
Daniel S. Robinson
drobinson@rcrsd.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

I. INTRODUCTION

Experian's attempt to shield basic *facts* concerning the 2015 data breach at issue in this case (the "Breach") from discovery by asserting those facts are either attorney-client communications or attorney work product must fail. Experian's business model relies, in large part, on collecting and analyzing the personally identifiable information ("PII") of its clients' customers—here, 15 million T-Mobile customers—in order to help its clients make customer application and credit decisions. Experian could not simply ignore the Breach's release of that PII to unauthorized parties; investigating the nature and extent of the Breach, and remediating it, are critical business responsibilities Experian had to perform regardless of whether a lawsuit ever was filed, just as it had done on prior occasions where it retained the same security vendor, Mandiant.

When Experian brought in Mandiant on September 21, 2015 (less than a week after learning of the Breach), to investigate and help remediate the Breach, it did so because its internal IT and Security departments lacked the "resources" to conduct the investigation and remediation internally. Experian's own IT and Security personnel had identified a potential cause of the Breach—a "weakness" in a vulnerable and outdated application on which its systems relied—but they needed Mandiant to determine which files and systems were affected, what types of PII were involved, how the Breach occurred, how to remediate the Breach, and what the required Breach notifications would state. Thus, Experian's pre-litigation decision to delegate its duties and responsibilities to investigate and remediate the Breach made Mandiant a percipient witness on the question of whether Experian's Breach investigation, remediation, and response met or fell below the standard of care. Further, as shown below, Mandiant's 2013 work *prior to the Breach* on the same Experian server at issue in the Breach is also relevant to whether Experian and/or Mandiant failed adequately to identify and remedy security vulnerabilities exploited in this Breach.

The Court denied, in part, Experian's motion to dismiss a variety of claims that Plaintiffs assert in this nationwide class action, including Plaintiffs' claim for negligence.

Plaintiffs are entitled to discovery on their negligence claim. However, Experian asserts that, because the law firm Jones Day filled out the paperwork to retain Mandiant, all of Mandiant's work and communications are privileged.

Simply put, Experian is using privilege arguments to withhold evidence related to its data breach vendor that is central to the truth-finding process in this case. Plaintiffs respectfully request that the Court order Experian to produce all documents listed on its most recent Privilege Log other than emails from, or solely to, Jones Day attorneys. Plaintiffs further request that the Court conduct an *in camera* review of certain additional documents in order to evaluate whether Jones Day's involvement was itself in the role of a percipient witness to Experian's investigation and remediation efforts, and whether, as such, those additional documents also should be produced to Plaintiffs.[1] In the alternative, Plaintiffs request that the Court conduct an *in camera* review of all the materials Experian listed on its Privilege Log.

II. BACKGROUND

A. The Data Breach, This Litigation, and Defendant's Assertions of Privilege

On October 1, 2015, Experian announced that it "experienced an unauthorized acquisition of information from a server" that held the PII of 15 million consumers in the United States, including those "who applied for T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015." (Dkt. 151, Compl. ¶ 1.) The PII involved in the "unauthorized acquisition" included the "names, dates of birth, addresses, and Social Security numbers and/or an alternative form of ID like a driver's license number, as well as additional information used in T-Mobile's own credit assessment." (*Id.*) Plaintiffs are consumers whose PII was acquired, accessed,

[1] The precise documents Plaintiffs request that the Court compel Experian to produce, or review *in camera*, are identified in the Notice of Motion and in the Proposed Order.

disclosed, and downloaded in the Breach, and, as a result of the Breach, they have suffered fraud, identify theft, financial harm, and a heightened, imminent risk of these harms.[2]

The first lawsuit based on the Breach was filed on October 2, 2015, and a number of such suits were consolidated in the present action on December 16, 2015. (Dkt. 60.) Plaintiffs requested that Experian produce the report of its forensic investigation of the Breach as part of its initial disclosures. (Dkt. 133 at 5.) However, Experian asserted the report was privileged at that time, and the parties raised the issue with the Court at a case management conference on March 31, 2016, at which time the Court ordered Experian to produce a privilege log concerning its forensic investigation. (3/31/2016 Tr. at 20.)

Experian produced its first privilege log on April 8, 2016. After Plaintiffs sent a letter in May describing the shortcomings of that log, Experian issued a Supplemental Privilege Log on June 10, 2016 that did not meaningfully address any of Plaintiffs' concerns. (Maya Decl. ¶¶ 2-5 & Ex. A (Supp. Priv. Log).)

The parties discussed Plaintiffs' intention to conduct a 30(b)(6) deposition focused on Experian's privilege assertions at subsequent case management conferences. (5/31/2016 Tr. at 6.) That deposition was conducted on February 9, 2017. (Maya Decl. Ex. B, Transcript of 2/9/17 Deposition of Richard Cannon ("Cannon Depo").)

Experian's 30(b)(6) witness, Richard Cannon, Vice President and Head of Corporate Security and Incident Response, was woefully unprepared. He had not viewed the full report, and was not certain what excerpts he had reviewed. (*Id.* at 57:6-8, 57:20-58:8, 188:4-6.) He could not even tell Plaintiffs the report's title, or describe, even in the most general fashion, any of the exhibits to it, which Experian had logged only as "one of eleven exhibits" each. (*E.g.*, Maya Decl. Ex. A (Priv Log) at P000037.) He also was unable to identify or describe any of the documents referenced on the privilege log. (*E.g.*,

[2] Experian has acknowledged that that the risks Plaintiffs face are real: "The information that was exposed could lead to an increased risk of identity theft," affected consumers should "be alert to 'phishing' by someone who acts like a colleague or friend and requests sensitive information over email," and "[c]onsider placing a fraud alert or security freeze on [their] credit file." Compl. ¶ 70.

Maya Decl. Ex. B (Cannon Depo) at 196:14-197:21, 202:6-203:9 (testifying he could not identify or describe an attachment to an email with regard to entry P19); *id.* at 191:19, 194:8-195:14 (testifying he could not identify or describe email he authored, which appeared on log, due to Defendant's redactions in version produced); 192:14-193:5 (testifying he did not help prepare the privilege log, only looked at a few documents listed in it in preparation for depo, and could not recall which ones).)

B. Experian Delegated Its Investigation to Mandiant, as It Had Done Before

Experian's discovery of the Breach and its retention of Mandiant preceded any lawsuit concerning it. On September 15, 2015, Experian employees Chris Kirby and Jason Leclair discovered high CPU usage on a server which appeared to be exporting data queried from another server through an intermediary server. (Maya Decl. Ex. C (EXP00132984-85, email re initial discovery of Breach).)

When responding to a data breach, a company must first ascertain the nature of that breach. (Strebe Decl. ¶ 21; Maya Decl. Ex. B at 30:17-31:4 (testifying that standard statements are created during the course of investigation and, in some cases, a report like Mandiant's); *id.* at 33:4-15 (testifying that, when an incident is serious, like the Breach in this case, Experian would either use an outside party that is contracted through their attorneys to do a forensic report/root-cause analysis, or develop its own report internally).) Experian's contract with T-Mobile required that, in the event of a breach, Experian must remedy, investigate, and remediate the breach. (Maya Decl. Ex. B at 238:21-239:24.) Indeed, Mr. Cannon testified that he has participated in similar investigations in the past, and that had Experian's security team been given sufficient "resources," it could have handled this investigation on its own; instead, Experian chose to conduct the investigation through Mandiant, in part because of the "resource issue." (*Id.* at 75:15-77:12, 77:24-25, 87:15-24.) Experian's IT and security personnel "ha[d] asked for resources for just general day-to-day work for this kind of thing for some time," specifying that "[i]t was manpower resources that we were asking for." (*Id.* at 78:21-24. 79:10-11.)

Upon learning of the Breach, Experian performed a preliminary review of the systems to determine the extent of the activity and how the activity occurred. (*Id.* at 48:24-49:12.) Without the assistance of an outside vendor, Experian "determined that [it] had an intruder in the environment" (*id.* at 45:15-19), that a "weakness" existed "in a [redacted] application" (*id.* at 50:18-24), and had developed "suspicions" concerning that affected application (*id.* at 51:16-52:2). Only after Mr. Cannon's team concluded that an attacker was in the system did they turned it over to "Legal." (*Id.* at 48:24-49:12.)

On September 21, 2015, Experian retained Mandiant, a third-party vendor and the market leader in such issues, through Jones Day to investigate the Breach. (*Id.* at 14:3-22, 66:20-24, 160:16-18.) Prior to that retention, Experian had worked with Mandiant frequently since 2007, either retaining Mandiant directly or through outside counsel. (*Id.* at 161:3-16, 163:8-10.) Experian also owned Mandiant products for several years (*id.* at 217:11-22), and had retained Mandiant to conduct initial security assessments for Experian on companies that Experian sought to acquire. (*Id.* at 141:12-142:10.) Experian also retained Mandiant to conduct investigations for past data breaches, similar to the one at issue here. (*Id.* at 214:5-14.) For instance, Experian retained Mandiant to investigate a suspected data breach in 2007 involving Experian's United Kingdom division. (*Id.* at 169:20-170:12.)

Experian previously retained Mandiant to investigate Decisioning Solutions, Inc., ("DSI") the company whose server later was involved in the Breach in this case, after Experian acquired that company. (*Id.* at 143:1-144:3.) Specifically, Experian retained Mandiant to investigate a 2013 data breach at DSI that involved the same networks compromised by the Breach in this case. (*Id.* at 147:3-7, 169:11-15, 172:17-25; 227:5-18; 228:14-229:17.) Around the time that Experian acquired DSI, Experian used Mandiant to investigate whether an unauthorized party accessed the PII of nearly 13,000 T-Mobile customers stored on DSI's servers. (*Id.* at 37:25-38:3, 165:8-166:4, 229:6-17.)

With respect to both the 2007 and 2013 data breaches, Mandiant prepared a report outlining data security issues, which Experian used to improve its data security. (*Id.* at

172:2-25.) Yet neither the 2007 breach nor the 2013 breach resulted in any litigation. (*Id.* at 214:5-14; 215:4-7.)

When Experian's internal IT and security teams turned over their initial findings concerning the 2015 Breach at issue in this case to Mandiant, Mandiant then identified which Experian business unit was breached and the specific files the unauthorized party acquired. (*Id.* at 52:12-53:3, 64:1-65:9, 179:8-181:2.) Experian and Mandiant then worked with T-Mobile to identify which T-Mobile customers had information in those files so that the scope of the required notice to affected consumers could be determined. (*Id.* at 65:10-66:19.) Experian, Mandiant, and T-Mobile then used that information to craft Experian's October 1, 2015 Data Breach announcement and notices to Plaintiffs and other putative class members. (*Id.* at 181:3-11.)

The vulnerability identified by Mr. Cannon and his team, which Mandiant further investigated, allowed the unauthorized party to use the [redacted] application to take over the application and access Plaintiffs' and putative Class members' PII. (*Id.* at 51:11-15.) One likely cause of this vulnerability is Experian's use of [redacted], a version released in 2004 that is widely known to be vulnerable to hacking. (Strebe Decl. ¶ 44.) Experian failed to update this version of [redacted] when it acquired DSI's servers in or around April 2013. (Maya Decl. Ex. B at 147:24-148:6, 165:8-166:4.)

No other formal report detailing Experian's investigation and remediation of the Breach—or lack thereof—exists. (*Id.* at 109:2-9; *see also id.* at 112:9-17 ("Q: Are you aware of any other report, aside from the vendor's report that was created in this case and relied upon by Experian for meeting their state and federal regulatory duties and responsibilities and other industry standards? A: I'm not aware of any reports, no.").)

C. Experian Has Taken the Position that Facts Concerning and Discovered Through Mandiant's Investigation Are Privileged

At the 30(b)(6) deposition, Experian's counsel made its position crystal clear: "whatever Mandiant did is going to be privileged." (*Id.* at 177:7-12.) Experian's assertions of privilege ignore one simple truth: Mandiant's actions are one and the same

as Experian's actions for purposes of liability in this case. Mandiant's investigation *was* Experian's investigation. Mandiant's remediation plan *was* Experian's remediation plan. Mandiant's Breach report *was* Experian's Breach report.

Experian's position that the Mandiant report, and its yet-to-be-identified eleven exhibits, are privileged does not change the fact Mandiant was a critical percipient witness to Experian's Breach response. Although Experian's counsel instructed its witness not to answer questions regarding the conclusions of the Mandiant report (*e.g.*, *id.* at 247:18-248:16 (instructing witness not to answer questions regarding conclusions of the Mandiant Report)), he permitted the witness to testify how significant portions of Experian's initial written notice to Plaintiffs and putative class members were based on those conclusions (*id.* at 179:2-184:1; Maya Decl. Ex. D (Depo Ex. 8, Experian's Press Release).) Critical evidence relevant to Experian investigation of the Breach and remediation have been concealed from discovery through Experian's assertion of privilege. (Maya Decl. Ex. B at 166:22-167:12 (instructing witness not to answer question about whether the [redacted] vulnerability associated with the 2015 Data Breach was previously identified by Mandiant in connection with its investigation of the 2013 data breach); *id.* at 61:2-25 (objecting to questions regarding what witness did to assist Mandiant in its investigation).)

While Experian refuses to disclose the Mandiant report to victims of its Breach, Defendant did disclose a redacted version of the report to T-Mobile. (*Id.* at 234:9-19; 243:22-25; Maya Decl. Ex. A at P000019-23 (emailing 8-page "draft report" to T-Mobile executive Dave Miller), P000059-63 (emailing 25-page "confidential report" to same), P000064-67 (emailing 7-page "confidential report" to same), P000091-93 (same), P000332-335 (emailing 25-page "final report" to same), P000335-39 (emailing 8-page "confidential report" to same).) Experian also delivered two versions of the full Mandiant report to its Board of Directors. (*Id.* at P000406-07 (showing transmission of 7-page and 25-page "final report[s]" to Experian's Board of Directors).)

Finally, the Mandiant report has become intertwined with the work of other percipient witnesses in the case. For example, Mr. Cannon testified that he and his team were asked to review and confirm the findings of the Mandiant report as part of their investigation and remediation efforts. (Maya Decl. Ex. B at 255:20-256:18.)

III. ARGUMENT

Experian cannot meet its burden of demonstrating that Mandiant's report and related documents are privileged or protected from discovery. Rather, as Mr. Cannon confirmed at the 30(b)(6) deposition, the Mandiant investigation (and its report) was Experian's only investigation and report concerning the basic facts of the Data Breach, is the only source of these facts, and such an investigation would have been required regardless of any then-yet-to-be-filed litigation. *See, e.g., Anderson v. Marsh*, 312 F.R.D. 584, 591 (E.D. Cal. 2015) (requiring disclosure where "[t]he purpose of the report is to determine what occurred during the incident and [how to respond]"). Indeed, Mr. Cannon himself testified he had generated such reports for Experian in the past, and would have done so here but for the fact that "the resource issue was taken care of by having an outside party do the work." (Maya Decl. Ex. B at 74:11-24.)

In any event, *facts* are not privileged, even when attorneys are copied on documents including them. *See, e.g.*, *Arfa v. Zionist Org. of Am.*, No. CV 13–2942 ABC, 2014 WL 815496, *5 (C.D. Cal. Mar. 3, 2014). Experian's assertions of the attorney-client privilege are meritless because Mandiant is a non-party that Experian retained for the business purpose of ascertaining what happened in the Breach and how to respond to it.

Experian's assertion of the attorney work product doctrine is equally inapplicable given that Mandiant's investigation was conducted, and its report prepared, to ascertain basic facts concerning the Data Breach, not because of anticipated litigation. *See, e.g.*, *U.S. v. Richey*, 632 F.3d 559, 568 (9th Cir. 2011) ("[W]here a document serves a dual purpose, that is, where it was not prepared exclusively for litigation, then the 'because of' test is used."); *Arfa*, 2014 WL815496, at *4 ("Documents prepared in the ordinary course

of business or that would have been created in essentially similar form irrespective of the litigation are not protectable as work product.") (citation omitted).

A. The Report Is Not Attorney Work Product

Experian cannot meet its burden of proving that the attorney work product doctrine applies to the Mandiant report. *Arfa*, 2014 WL 815496, at *2. "To qualify for work-product protection, documents must: (1) be 'prepared in anticipation of litigation or for trial' and (2) be prepared 'by or for another party or by or for that other party's representative.'" *Richey*, 632 F.3d at 567 (citation omitted). "'At its core, the work product doctrine shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case.'" *Ward v. Equilon Enters., LLC*, No. 9-4565, 2011 WL 2746645, at *2 (N.D. Cal. July 13, 2011) (quoting *United States v. Nobles*, 422 U.S. 225, 238-39 (1975)).

The doctrine's protections are waivable. *Richey*, 632 F.3d at 567. Furthermore, the doctrine's protections are not absolute; rather, "[w]ork product material that concerns factual matters may be discovered if the party seeking it demonstrates a 'substantial need' for the material and there is no other means for obtaining that information without undue hardship." *In re EHR Aviation, Inc.*, No. 16-mc-80093-JCS, 2016 WL 5339802, *7 (N.D. Cal. Sept. 23, 2016) (quoting Fed. R. Civ. P. 26(b)(3)(A)); *see also Arfa*, 2014 WL 815496, at *4 (explaining how "'[o]rdinary' work product includes 'raw factual information,'" and may "be discovered if the party seeking the discovery demonstrates a 'substantial need' for the materials and there is no other means for obtaining that information without undue hardship") (citations omitted).

1. Experian's Investigation Would Have Been Conducted, and the Report Would Have Been Prepared, Regardless of any Threat of Litigation

The proposition that, absent the threat of this litigation, Experian would not have investigated the Breach, determined whose information was stolen, or prepared any report concerning that investigation is absurd. Experian is one of the three largest credit bureaus, and touts itself as a leader in data breach response. Experian's own Data Breach Response

Guide, which it publishes annually, even suggests that companies conduct an investigation similar to the one that it conducted here. (Maya Dec. Ex. E (Experian's 2016-2017 Data Breach Response Guide) at 8 ("Forensics partners need to have the ability to clearly translate technical investigations into what the enterprise risk implications are of a data breach for decision-makers within the organization.").)

Any argument by Experian that it only conducted this investigation because of the threat of litigation is clearly an attempt to hide the investigation's findings as privileged. As it acknowledges, Experian is permitted to collect and use PII like that obtained by hackers during this Breach because it "is held accountable for its information use by consumer privacy expectations and by laws and industry codes established by government entities and industry organizations around the world," including laws such as the Fair Credit Reporting Act ("FCRA") and the Gramm-Leach-Bliley Act ("GLBA"). (Compl. ¶ 76 (quoting Experian's privacy policy).) The GLBA imposes on Experian "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. Similarly, the FCRA requires Experian to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under . . . this title." 15 U.S.C. § 1681e(a).[3]

As Plaintiffs' expert notes: "A data breach investigation and report is a critical and necessary starting place for any data breach resolution, because such a report identifies the affected systems that must be repaired." (Strebe Decl. ¶ 21.) Experian's 30(b)(6) witness admitted that Experian always investigates such data breaches. (Maya Decl. Ex. B at 30:17-31:4 (testifying standard statements are created during the course of investigation and, in some cases, a report like Mandiant's); *id.* at 33:4-15 (testifying that, when an incident is serious, like the Breach here, Experian would either use an outside

[3] Although the Court dismissed Plaintiff's FCRA claim, it does not follow that Experian could have chosen not to ascertain the nature of, and remediate, the Breach without running afoul of its responsibilities as a consumer reporting agency.

party that is contracted through their attorneys to do a forensic report/root-cause analysis, or would develop its own report internally).)

Mandiant investigated this Breach because Mr. Cannon's team lacked the resources to conduct such an extensive investigation itself. (Maya Decl. Ex. B at 74:11-24 (testifying that Mr. Cannon's team could not conduct the investigation on their own because of a "resource issue").) Mr. Cannon explained that his "team is small," and that it "takes extensive investigation to do that type of work." (*Id.* at 75:3-5.) When asked whether he requested additional resources to conduct the investigation, Cannon asserted that "[t]he resource issue was taken care of by having an outside party do the work." (*Id.* at 77:19-25.) As such, Mandiant did not investigate and create its report in anticipation of litigation—rather, Experian retained Mandiant because its own data security team lacked sufficient resources to investigate the Breach. Had Experian provided Mr. Cannon's team with the necessary resources, it is not only likely that the Breach may not have occurred, but that it would have investigated the Breach without using Mandiant.

Experian's prior practice of retaining Mandiant to respond to data breaches when such incidents did not result in litigation further demonstrates that Experian would have prepared these materials regardless of any threat of litigation.[4] Similarly, the fact that Experian presented two versions of the Mandiant report to its board of directors suggests that these materials "resemble business documents rather than documents prepared in

[4] Maya Decl. Ex. B at 161:3-16, 163:8-10 (testifying that Experian worked with Mandiant frequently since 2007, either directly or through Jones Day); *id.* at 214:5-14 (testifying Experian retained Mandiant to conduct investigations for past data breaches, similar to the one at issue here); *id.* at 169:20-170:12 (testifying Experian retained Mandiant investigate a suspected data breach in 2007 involving Experian's United Kingdom division); *id.* at 147:3-7, 172:17-25 (testifying Experian retained Mandiant to investigate the 2013 data breach involving the same networks compromised by the breach in this case); *id.* at 172:2-25 (testifying that Mandiant prepared a report concerning its investigations of both the 2007 and 2013 data breaches); *id.* at 214:5-14 (testifying that neither the 2007 nor the 2013 breach resulted in litigation).

anticipation of litigation." *Southern Union Co. v. Southwest Gas Corp.*, 205 F.R.D. 542, 549 (D.Ariz. 2002); *Arfa*, 2014 WL 815496, at *4 (quoting same).

Mr. Cannon testified that it was Mandiant who determined the Breach at issue "was limited to the T-Mobile customers" (*id.* at 46:19-21), it was Mandiant who determined that Experian's credit bureau was not affected (*id.* at 179:19-23), and it was Mandiant who "told us what files had been taken" (*id.* at 64:16-65:7). Any contention that Experian only endeavored to reach such basic conclusions regarding the Breach because of the threat of litigation, or that the investigation and its conclusions are therefore protected from discovery, is untenable. It is absurd to think that Experian, a self-proclaimed leader in responding to data breaches, would have chosen not to investigate the Breach, not to remediate the Breach, or not to inform the victims of the Breach that their data had been stolen, as required by laws such as Cal. Civ. Code § 1798.82.

As described in Section II.B above, Mandiant's investigation and report were the only such investigation conducted, and report produced, concerning the Breach. Mandiant's investigation and report provided the basis for many of Experian's public statements concerning the Breach, including those it included in the initial notice it provided to Plaintiffs and other putative class members, as required by state data breach laws like Cal. Civ. Code § 1798.82. (*Id.* at 179:2-184:1.)

2. <u>Plaintiffs Have a Substantial Need for the Mandiant Report</u>

Plaintiffs cannot access Experian's systems as they existed at the time of the Breach or conduct an investigation of those systems in a manner comparable to the access and means that Mandiant had when it performed its investigation. (Strebe Decl. ¶¶ 20-52.)

Although Experian's witness testified that it captured digital images of "affected systems," it was Mandiant's analysis that determined which systems were so "affected," and such files are totally inadequate to perform an investigation like Mandiant's. (*Id.* at ¶¶ 27-33.) "Many other systems that Mandiant may not have identified as 'affected' would have been 'involved' in the data breach," and viewed and accessed in the course of Mandiant's investigation. (*Id.* at ¶ 33.)

Indeed, Experian does not and cannot contend that Mandiant could or would rely on such images, captured by another entity of what that entity concluded, through secret means, were the only "affected" systems, to conduct such an investigation in the first instance. Rather, in the experience of Plaintiffs' expert, such investigations by Mandiant typically are "performed primarily on the live, operational network." (*Id.* at ¶ 32.)

> [I]t is exceptionally common for attackers to "move through" networked systems and devices without affecting their operation, accessing data and accounts on those systems for purposes such as elevating the attackers' access privileges, obtaining stored passwords, switching accounts, and proxying their connections through intermediate systems to the ultimate systems targeted. These intermediate systems provide evidence of what occurred but are not considered "affected" because they require no remediation work.

(Strebe Decl. ¶ 34.) Indeed, evidence suggests this is exactly how the Breach occurred. (Maya Decl. Ex. C.) "Mandiant's goal would have been remediation of the Breach, not creating a recipe to recreate its own investigation." (Strebe Decl. at ¶ 33.)

As Plaintiffs' expert declares, "[t]he data needed to produce a report like the Mandiant data breach report in this case would not exist today." (*Id.* at ¶ 25.) "To the extent efforts have been made to preserve such data, that data will not exist in the same state or in the same context that it existed at the time of the data breach at issue." (*Id.*) For example, "[i]t is highly likely that necessary log files were deleted during the process of remediating the Breach." (*Id.* at ¶ 26.)

Experian's witness testified that it retained Mandiant to perform its investigation here because its internal IT department lacked sufficient resources to conduct the investigation on its own. (Maya Decl. Ex. B at 81:14-19.) Yet Experian appears to contend that Plaintiffs could perform such an investigation, some two years after the Breach, by relying only on whatever stale evidence Experian may have chosen to preserve (though it has not yet produced any such evidence), knowing that this is not how Mandiant could or would have conducted its investigation. "Any equivalent investigation would

need exactly the same level of access as Mandiant had to the live systems at the same moment in time." (Strebe Decl. ¶ 31.)

The Mandiant investigation was Experian's response to the Breach. It is evidence that goes directly to Plaintiffs' claims in this action, including the claim that the Breach was a predictable consequence of Defendant's negligence. (*E.g.* Strebe Decl. ¶¶ 39-47 (addressing Defendant's use of an outdated version of an application with widely known security flaws at the time of the breach).) As explained by Plaintiffs' expert, Mandiant's prior investigation of the DSI data breach in 2013 "places Mandiant in a position where it could fully grasp Experian's data security network, including Experian's continued use of [redacted] in 2015, and any changes Experian made to its data security network between 2013 and 2015 that may have caused the Breach." (*Id.* at ¶ 48.) As many of the vulnerabilities, such as use of [redacted], that led to the Breach were carried over from those servers that Mandiant previously investigated, significant concerns exist as to whether Mandiant negligently investigated the servers in 2013, or whether Experian ignored known risks that Mandiant's 2013 report identified. (*Id.* ¶ 41.) Clearly, Plaintiffs have a substantial need for the Mandiant report, and would be entitled to production of this evidence in discovery even if the report were considered attorney work product (which it is not for the reasons described in the preceding section).

B. <u>The Report Is Not Protected by the Attorney-Client Privilege</u>

An eight-part test determines whether information is covered by the attorney-client privilege:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection be waived.

U.S. v. Ruehle, 583 F.3d 600, 607 (9th Cir. 2009) (quoting *In re Grand Jury Investigation*, 974 F.2d 1068, 1071 n.2 (9th Cir.1992)); *Richey*, at 566 (same). As with

the attorney work product doctrine, "[t]he party asserting the privilege bears the burden of proving each essential element." *Ruehle*, 583 F.3d at 607.

1. Mandiant's Investigation Was Not Conducted, and Its Report Was Not Produced, Because of Any Need for Legal Advice

As described above, the Mandiant investigation and report constituted Experian's initial response to the Breach. As such, this material is basic factual evidence, and it is an abuse of the privilege to claim the material constitutes, primarily, "legal advice." *Id.*; *see also Richey*, 632 F.3d at 566 ("If the advice sought is not legal advice, but, for example, accounting advice from an accountant, then the privilege does not exist.").

Jones Day willingly chose to tread "the treacherous path which corporate counsel must tread under the attorney-client privilege when conducting an internal investigation." *Ruehle*, 583 F.3d at 601. But the firm's choice to take on this role does not and cannot confer privileged status on the facts surrounding this data breach, which Experian now seeks to hide. Although Jones Day inserted itself into the investigation at an early stage in an attempt to confer privileged status on the subsequent investigation and report, this only puts the firm in the uncomfortable position of a percipient witness, which necessarily conflicts with the firm's current position as Experian's outside counsel of record in this litigation—not a conflict of Plaintiffs' making.

"That a person is a lawyer does not, *ipso facto*, make all communications with that person privileged. The privilege applies only when legal advice is sought 'from a professional legal advisor *in his capacity as such*.'" *United States v. Chen*, 99 F.3d 1495, 1501 (9th Cir. 1996) (citation omitted) (italics in original); *see also Ruehle*, 583 F.3d at 607 ("The fact that a person is a lawyer does not make all communications with that person privileged.") (citations omitted). Just as advice from a lawyer concerning "investment opportunities" is not privileged, so too is Jones Day's assistance in ascertaining the nature of the Breach and how to respond, in a technical sense, not privileged. *Chen*, 99 F.3d at 1501 (quoting and referring to *Liew v. Breen*, 640 F.2d

1046, 1050 (9th Cir. 1981) (holding communications with lawyer "with the aim of finding meritorious litigation to finance" not privileged)).

As the Ninth Circuit observed in *Ruehle*, when it reversed a district court's decision to shield a corporate executive's statements to the corporation's counsel during an internal investigation into stock option backdating from discovery:

> "Because it impedes full and free discovery of the truth, the attorney-client privilege is strictly construed." . . . "[T]he privilege stands in derogation of the public's 'right to every man's evidence' and as 'an obstacle to the investigation of the truth,' [and] thus, ... '[i]t ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle.'"

Ruehle, 583 F.3d at 607 (citations omitted).

Unlike Jones Day, Mandiant is not a law firm. While "[t]he privilege also protects communications involving agents of the attorney," it does so only to the extent such communications are "in furtherance of the attorney-client relationship." *Arfa*, 2014 WL 815496, at *5. And while the privilege protects "the 'disclosure of *communications* between the attorney and the client[,] it does not protect disclosure of underlying facts which may be referenced within a qualifying communication.'" *Id.* (quoting *State Farm Fire & Casualty Co. v. Superior Court*, 54 Cal. App. 4th 625, 639 (1997)) (italics in original). As established above, the Mandiant investigation and report were Experian's initial response to the Breach and, as such, this is factual material, not "communications" between Jones Day and Experian "in furtherance of the attorney-client relationship." *Arfa*, 2014 WL 815496, at *5; *see also id.* ("'[D]ocuments prepared independently by a party, including witness statements, do not become privileged communications or work product merely because they are turned over to counsel.'") (quoting *Wellpoint Health Networks, Inc. v. Superior Court*, 59 Cal. App. 4th 110, 119 (1997)).

Moreover, while Jones Day, unlike Mandiant, is a law firm, its involvement in the required investigation and remediation of the Breach is not necessarily privileged. Just

as an employer cannot simultaneously argue, in a workplace harassment case, that it investigated the alleged harassment as required by law, and that the investigation is privileged because it was performed by a lawyer, so too has Experian waived any claim of privilege it now asserts with respect to Jones Day's involvement in Experian's required investigation and remediation of the Breach. *See*, *e.g.*, *Richey*, 632 F.3d at 566-68 (rejecting claim of privilege and work product protection concerning valuation report prepared at request of attorney); *Ward v. Equilon Enters., LLC*, No. 9-4565, 2011 WL 2746645, at *2 (N.D. Cal. July 13, 2011) (rejecting claim of privilege regarding investigation and report produced by attorney to satisfy requirements of California law regarding workplace safety).

Experian likely hoped to shield this evidence from discovery by engaging Mandiant through Jones Day, but this does not transform Mandiant's technical work of ascertaining the nature of the Breach and how to respond from a necessary business activity into an attorney-client communication immune from discovery. *See, e.g.*, *Liew*, 640 F.2d at 1050. Rather, Jones Day's involvement raises serious questions about whether *any* of its communications with Mandiant or with Experian concerning the Mandiant investigation can be considered privileged. While Plaintiffs are not seeking to compel production of every document Experian listed on its privilege log concerning the Mandiant report, they seek production of any such document that, based on the log, constitute communications between Experian and Mandiant, and Plaintiffs further request that the Court conduct an *in camera* review of certain documents that, although they appear to be communications from Jones Day, may in fact relate to non-privileged, technical issues concerning Experian's response to the Breach, rather than legal advice.[5]

[5] These documents are referenced in the notice of motion and [proposed] order, and include entries such as a document that listed as authored by "Jones Day," and described in vague terms as a "[c]onfidential memorandum providing legal advice and prepared in anticipation of litigation re: summary of undisclosed experts' analysis and investigation of breach, attached to privileged email chain." Maya Decl. Ex. A at P000249. Plaintiffs

2. Experian's Privilege Log Does Not Support Its Privilege Assertions

Under the Federal Rules, "[w]hen a party withholds information otherwise discoverable by claiming that the information is privileged," that party must "expressly" assert the privilege and describe the nature of the information "in a manner that . . . will enable other parties to assess the claim." Fed. R. Civ. P. 26(b)(5).

Where a party relies on a "conclusory privilege log" such as that on which Experian relies here (Maya Decl. Ex. A), a court will "find a document privileged only where the attorney-client privilege and/or work-product doctrine obviously applies based on the face of the document itself." *E.E.O.C. v. Safeway Store, Inc.*, No. C–00–3155 TEH(EMC), 2002 WL 31947153, *3 (N.D. Cal. Sept. 16, 2002). None of Experian's current entries regarding attachments to emails justify withholding the referenced documents. *See Arfa*, 2014 WL 815496, at *1 ("[S]imply copying or sending materials to an attorney does not automatically convey protected status over those materials.").

During the specially held 30(b)(6) deposition focused entirely on, and expressly limited to, Experian's claims of privilege, Experian's witness could provide no additional basis for Defendant's privilege assertions. The witness was unable to describe, even generally, a single exhibit to the Report, and Defendant describes them only as "one of eleven exhibits" on the log itself. (*E.g.*, Maya Decl. Ex. A (Priv Log) at P000037.) Similarly, the witness testified he had not personally reviewed the report itself, and he was unable to provide such basic—and obviously unprivileged—information as the report's title. (Maya Decl. Ex. B at 247:7-10, 248:17-249:5.)

C. Any Claim of Attorney-Client Privilege or Work Product Protection Was Waived Through Disclosure to Third Parties

As mentioned above, both the protections of both the attorney-client privilege and the work product doctrine can be waived. "[V]oluntarily disclosing privileged documents

---

ask the Court to conduct an *in camera* review of this document and other, similar entries because, based on the privilege log, it appears that the document may concern Mandiant's investigation rather than actual legal advice.

to third parties will generally destroy the privilege." *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1126-27 (9th Cir. 2012).

Here, Experian disclosed selected conclusions from Mandiant's investigation and report to the world, including directly to Plaintiffs, in its initial notices concerning the Breach.[6] Experian cannot both assert that the Breach did not affect its credit bureau business, based on Mandiant's investigation and findings, while continuing to claim that these materials are privileged and protected from discovery. *See, e.g.*, *Arfa*, 2014 WL 815496, at *6 (explaining how "a party waives the attorney-client privilege if it 'has disclosed a significant part of the communication or has consented to such disclosure made by anyone'") (quoting Cal. Evid. Code § 912(a)); *Wellpoint Health Networks*, 59 Cal. App. 4th at 128 ("[W]aiver is established by a showing that 'the client has put the otherwise privileged communication directly at issue and that disclosure is essential for a fair adjudication of the action.'") (citation omitted).

Experian disclosed multiple versions of the Mandiant report to T-Mobile, to whom Experian may well be liable for failing to safeguard the PII of T-Mobile's customers.[7] Experian asserts this disclosure does not constitute a waiver because it has a joint defense agreement with T-Mobile. (*E.g.*, Maya Decl. Ex. A (Priv Log) at P000019 (referring to joint defense agreement).) Experian has not produced that joint defense agreement, despite Plaintiffs' requests, but such an agreement does not automatically satisfy Experian's burden of establishing that such communications with a potential adversary remain privileged. *See, e.g., In re Pac. Pictures Corp.*, 679 F.3d at 1128-29 (rejecting

---

[6] Maya Decl. Ex. D at 1 ("This incident did not impact Experian's consumer credit database"); Maya Decl. Ex. B at 179 (testifying this statement was based on Mandiant's investigation); Maya Decl. Ex. F (Experian's notice to Plaintiffs) at EXP-PLTFS-000001 ("This did not involve access to Experian's credit reporting database.").

[7] Maya Decl. Ex. A (Priv Log) at P000019-23 (emailing 8-page "draft report" to T-Mobile executive Dave Miller), P000059-63 (emailing 25-page "confidential report" to same), P000064-67 (emailing 7-page "confidential report" to same), P000091-93 (same), P000332-335 (emailing 25-page "final report" to same), P000335-39 (emailing 8-page "confidential report" to same).

attempt to rely on letter from US Attorney's Office to preserve privilege claim despite disclosure to the government). Plaintiffs do not name T-Mobile as a defendant in this action, and it is clear that Experian and T-Mobile have different and conflicting interests with respect to the issues raised here.

Experian waived any claim that the Mandiant materials are protected from discovery by the attorney-client privilege or by the attorney work product doctrine by disclosing those materials to T-Mobile and by disclosing selective portions to the world and to Plaintiffs directly in Experian's public statements concerning the Breach.

IV. CONCLUSION

For all these reasons, Plaintiffs respectfully request that the Court grant this motion and order Experian to produce the documents referenced in the Notice of Motion and in the Proposed Order to Plaintiffs immediately. Plaintiffs further request that the Court conduct an *in camera* review of the additional documents also identified in the Notice and in the Proposed Order, and similarly order those documents be produced to Plaintiffs should the Court conclude, after its review, that Experian's claims of privilege regarding those documents are not well taken.

Dated: April 12, 2017

Respectfully submitted,

AHDOOT & WOLFSON, P.C.

/s/ Theodore Maya

Tina Wolfson
twolfson@ahdootwolfson.com
Theodore Maya
tmaya@ahdootwolfson.com
1016 Palm Avenue
West Hollywood, CA 90069
Telephone: 310-474-911
Fax: 310-474-8585

ROBINSON CALCAGNIE ROBINSON SHAPIRO DAVIS, INC.

/s/ Daniel S. Robinson
Daniel S. Robinson
drobinson@rcrsd.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

Plaintiffs' Interim Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on April 12, 2017, I caused to be filed the foregoing document. This document is being filed electronically using the Court's electronic case filing (ECF) system, which will automatically send a notice of electronic filing to the email addresses of all counsel of record.

Dated: April 12, 2017

/s/ Daniel S. Robinson
Daniel S. Robinson